Configuring BaySecure FireWall-1

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 117384-A Rev A
September 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. September 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BayStream, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Before You Begin xi
Conventions xii
Acronyms xii
Ordering Bay Networks Publications xiii
Bay Networks Customer Service xiii
How to Get Help xiv

Chapter 1
BaySecure FireWall-1

Obtaining a FireWall-1 License 1-2
Installing and Running the FireWall-1 Management Software 1-3
Installing on the UNIX Platform 1-3
Mounting the CD and Extracting the Tar File 1-3
Installing the Check Point FireWall-1 Software 1-4
Installation Options 1-4
Sample Installation 1-5
Customizing the FireWall-1 Installation 1-8
Installing a License on the Management Station 1-9
Starting and Stopping the FireWall-1 Daemons 1-9
Synchronizing the Management Station and the Router Passwords 1-9
Starting the FireWall-1 GUI 1-10
Installing on the Windows/NT Platform 1-10
Sample Installation 1-10
Customizing the FireWall-1 Installation 1-17
Creating and Configuring a FireWall on the Router 1-17
Enabling the FireWall on All Router Interfaces 1-21
Activating the Firewall 1-22
Configuring a FireWall Security Policy 1-24

Installing the Security Policy on the Router 1-24
Troubleshooting Checklist 1-25
Index

Figures

Figure 1-1. Choose Destination Location Window 1-11
Figure 1-2. Selecting Product Type Window 1-11
Figure 1-3. Licenses Window 1-12
Figure 1-4. Administrators Window 1-13
Figure 1-5. Add Administrators Window 1-13
Figure 1-6. Hit Key Session Window 1-14
Figure 1-7. CA Key Window 1-15
Figure 1-8. Choose Destination Location Window 1-16
Figure 1-9. Select Components Window 1-16
Figure 1-10. Configuration Manager Window 1-18
Figure 1-11. F.W. Global Window 1-19
Figure 1-12. F.W. Router Parameters Window 1-20
Figure 1-13. FW on ALL Interfaces Window 1-21
Figure 1-14. Boot Router Window 1-23

About This Guide

If you are responsible for network security, you need to read this guide to learn about BaySecure FireWall-1, and the steps you need to take to install, configure, and activate a firewall on a Bay Networks® router.

If you want to	Go to
Obtain a Check Point FireWall-1 license	page 1-2
Install Check Point firewall management software	page 1-3
Create and configure a firewall on the router	page 1-17
Enable the firewall on all router interfaces	page 1-21
Activate the firewall	page 1-22
Configure a security policy	page 1-24
Install the security policy on the router	page 1-24

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks® Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–11.xx to Version 12.00*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20

Acronyms

GUI	graphical user interface
IP	Internet Protocol
LAN	local area network
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 508-916-8880 (direct)	508-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	508-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1
BaySecure FireWall-1

BaySecure™ FireWall-1 integrates version 2.1 of Check Point Software Technologies Ltd™ FireWall-1™ software, with the exception of user authentication, address translation, statistics and encryption features, into the Bay Networks GAME router operating system. The result is a security system that provides fully secure, bidirectional, anti-spoofing communication for all Internet applications and services, such as FTP, Telnet, and SMTP.

The Check Point FireWall-1 software consists of these two modules:

- *Firewall module* -- the firewall module inspects all data packets traveling between the data link and network layers, and either forwards or drops them according to the security policy you specify. It also provides communication between the firewall module and the control module. Bay Networks integrates the firewall module into the router operating system.
- *Control module* -- the control module allows you to manage the firewall and to define a security policy. The security policy determines the rules the FireWall-1 software uses to determine whether to let data pass or to log an error and alert the management station. The control module resides on a workstation, called the firewall management station.

For detailed information about the Check Point FireWall-1 software, refer to your Check Point documentation.

To configure a firewall on a router, see the following sections:

- Obtaining a FireWall-1 License on 1-2
- Installing and Running the FireWall-1 Management Software on 1-3
- Creating and Configuring a FireWall on the Router on 1-17
- Enabling the FireWall on All Router Interfaces on 1-21
- Activating the Firewall on 1-22
- Configuring a FireWall Security Policy on 1-24
- Installing the Security Policy on the Router on 1-24

Obtaining a FireWall-1 License

Before you can install the Check Point FireWall-1 software and create a firewall on the router, you must first obtain a FireWall-1 license. You need a separate FireWall-1 license for each router. To obtain a license:

1. **Locate your license certificate.**

   A FireWall-1 license certificate accompanies the Check Point FireWall-1 software media. On the license certificate you will find a FireWall-1 serial number. You must have your serial number to obtain a FireWall license.

   If you lose the license certificate bearing the FireWall-1 serial number, contact Bay Networks.

2. **Contact Check Point.**

   To obtain a permanent license, you must contact Check Point. You can reach Check Point

   - Via the world wide web at **http://license.CheckPoint.com**
   - By sending mail to license@checkpoint.com
   - By phoning Check Point:

     800-429-4391 (North America)

     +972-3-613-1833 (outside North America)

   When requesting a license, you must provide the serial number from the license certificate, as well as information, such as IP addresses, regarding the end user and the hosts on which you plan to install the FireWall-1 software.

Note: If you need to change the IP address of the FireWall-1 management station, contact Check Point at 800-429-4391 (North America) or +972-3-613-1833 (locations outside of North America).

Refer to the section "Installing and Running the FireWall-1 Management Software" and the Check Point documentation for information about how to install the license.

Installing and Running the FireWall-1 Management Software

Once you obtain a FireWall-1 license from Check Point, you can install the Check Point FireWall-1 management software on either the UNIX or Windows/NT platform.

Installing on the UNIX Platform

Before you install the Check Point software, be sure to

- Contact Check Point to get a license
- Add **setenv FWDIR/etc/fw** to your *.cshrc* file, or add **FWDIR=/etc/fw** to your *.cshrc* file and export FWDIR to your *.profile* file
- Add **/etc/fw/bin** to your path
- Add **/etc/fw/man** to your MANPATH environment

Use the following sections as a guide to installing the FireWall-1 software on the UNIX platform. For more details, refer to your Check Point documentation.

Mounting the CD and Extracting the Tar File

Check Point supplies its FireWall-1 software on CD-ROM. You must mount the CD drive and extract the tar files.

Commands used to mount a CD drive and extract the tar files vary depending the device name of the CD drive, the operating system used, and other environmental factors. Use the instructions that follow only as guidelines for mounting the CD drive and extracting the tar files. The commands you need may differ.

For SunOS

```
lab#  mount -r -t hsfs /dev/sr0 /cdrom
lab#  cd /tmp
lab#  tar xvf /cdrom/sunos4/fw1/fw.sunos4.tar
```

For Solaris

```
lab#  mount -F hsfs -r /dev/sr0 /cdrom
lab#  cd /tmp
lab#  tar xvf /cdrom/solaris2/fw1/fw.solaris2.tar
```

For HPUX

```
lab#  mount -r /dev/dsk/c1t2d0 (or your specific CD-ROM address)  /cdrom
lab#  cd /tmp
lab#  tar xvf  "/cdrom/HPUX/FW1/FW.HPUX.TAR;1"
```

Installing the Check Point FireWall-1 Software

Once you have extracted the Check Point FireWall-1 files, you can install the management software. To install the software, change directories so that you're in the directory where you put the files and then issue the **fwinstall** command.

For example, if you extracted the files into your */tmp* directory, install the software by issuing the following commands:

```
lab#  cd /tmp
lab#  ./fwinstall
```

Installation Options

Note that during the installation, the script asks you to select the FireWall-1 option you want to install. To be compatible with BaySecure FireWall-1, enter selection 3, FireWall-1 Enterprise Management Console Product. A sample follows.

```
Which of the following FireWall-1 options do you wish to install?

(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-7/a): 3
```

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD-ROM and installs it onto a SparcStation running SunOS. Use this sample installation to familiarize yourself with the FireWall-1 installation script.

Note: In the following sample installation, all user input is in **bold**.

```
*************** FireWall-1 v3.0 Installation ***************

Reading fwinstall configuration.  This might take a while.
Please wait.

Configuration loaded.  Running FireWall-1 Setup.

Checking available options. Please wait.....................

Which of the following FireWall-1 options do you wish to
install/configure ?
------------------------------------------------------------------------
(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-5/a): 3

Installing/Configuring FireWall-1 Enterprise Management Console Product.

Please wait...

Selecting where to install FireWall-1
--------------------------------------
FireWall-1 requires approximately 9017 KB of free disk space.
Additional space is recommended for logging information.

Enter destination directory [/etc/fw]): <RETURN>

Checking disk space availability...

Installing FW under /etc/fw (50836 KB free)
Are you sure (y/n) [y] ? y
```

```
Software distribution extraction
--------------------------------
Extracting software distribution. Please wait ...
Software Distribution Extracted to /etc/fw
Installing license
------------------
Reading pre-installed license file fw.LICENSE... done.

The following evaluation License key is provided with this FireWall-1
distribution
Eval            15Mar97    3.x pfmx controlx routers connect motif

Do you want to use this evaluation FW-1 license (y/n) [y]? n

Do you wish to start FireWall-1 automatically from /etc/rc.local (y/n)
[y] ? n


Welcome to FireWall-1 Configuration Program
===========================================
This program will guide you through several steps where you
will defined your FireWall-1 configuration. In any later time,
you can reconfigure these parameters by running fwconfig


Configuring Licenses...
=======================
The following licenses are installed on this host:
Eval            15Mar97    3.x pfmx controlx routers connect motif

Do you want to add licenses (y/n) [n] ? n


Configuring Administrators...
=============================
No FireWall-1 Administrators are currently defined for this Management
Station.

Do you want to add users (y/n) [y] ? n


Configuring GUI clients...
==========================
GUI clients are trusted hosts from which FireWall-1 Administrators are
allowed to log on to this Management Station using Windows/X-Motif GUI.

Do you want to add GUI clients (y/n) [y] ? n
```

```
Configuring Remote Modules...
=============================
Remote Modules are FireWall or Inspection Modules that are going
to be controlled by this Management Station.

Do you want to add Remote Modules (y/n) [y] ? n

Configuring Groups...
=====================
FireWall-1 access and execution permissions
-------------------------------------------
Usually, FireWall-1 is given group permission for access and execution.
You may now name such a group or instruct the installation procedure
to give no group permissions to FireWall-1. In the latter case, only the
Super-User will be able to access and execute FireWall-1.

Please specify group name [<RET> for no group permissions]:

No group permissions will be granted. Is this ok (y/n) [y] ? y

Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used for
generating Certificate Authority RSA keys.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [                   ] *

Thank you.

Configuring CA Keys...
======================
fw: no license for 'ca'
The installation procedure is now creating an FWZ Certificate Authority
Key
for this host. This can take several minutes. Please wait...
fw: no license for 'ca'

Configuration ended successfully

*************** FireWall-1 is now installed. ***************
```

```
Do you wish to start FW-1 now (y/n) [y] ? n
*****************************************************************
Configuration ended successfully

*************** FireWall-1 is now installed. ***************

Do you wish to start FW-1 now (y/n) [y] ? n

*****************************************************************
               DO NOT FORGET TO:
1. add the line:    setenv FWDIR /etc/fw   to .cshrc
               or  FWDIR=/etc/fw; export FWDIR to .profile
2. add  /etc/fw/bin  to path
3. add  /etc/fw/man  to MANPATH environment
*****************************************************************

You may configure FireWall-1 anytime, by running fwconfig.

*************** Installation completed successfully ***************
```

Customizing the FireWall-1 Installation

You can use the **fwconfig** command to customize your FireWall-1 installation. Using **fwconfig**, you can add

- A license
- Administrators
- GUI clients
- Remote modules
- Groups
- CA keys

Note: To add an administrator, you must first add a group to which the user is a member. If you do not add a group, then you can run the GUI using only the **fwui** command if you are logged in as root.

Refer to your Check Point documentation for details.

Installing a License on the Management Station

To install a license on the management station, use the following command:

fw putlic *<hostid> <lic_string>* pfmx controlx routers motif embedded

The <*hostid*> is the host ID of the management station.

The <*lic_string*> is a string of alphanumeric characters that Check Point provides when you request your FireWall-1 license.

Starting and Stopping the FireWall-1 Daemons

To start the FireWall-1 daemons, use the **fwstart** command. For example, at the system prompt, type

```
lab# fwstart
```

To stop the FireWall-1 daemons, use the **fwstart** command. For example, at the system prompt, type

```
lab# fwstop
```

Synchronizing the Management Station and the Router Passwords

Once you have installed licenses on the management station and the router, you must synchronize your password on the two systems. To synchronize the router and the management station passwords, enter the following commands:

- On the firewall management station:

  fw putkey -p*<password> <ip_address_fwall_router>*

- On the router:

  fwputkey *<password> <ip_address_mgmt_station>*

  where

<password>	is a string of alphanumeric characters that comprise your password
<ip_address_fwall_router>	is the IP address of your firewalled router
<ip_address_mgmt_station>	is the IP address of your FireWall-1 GUI management station

Starting the FireWall-1 GUI

To start the FireWall-1 GUI, enter the **fwui&** command. For example, at the system prompt, type

```
lab# fwui&
```

Installing on the Windows/NT Platform

Use the following sections as a guide to installing the FireWall-1 software on the Windows/NT platform. For more details, refer to your Check Point documentation.

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD-ROM and installs it onto a PC running Windows/NT. Use this sample installation to familiarize yourself with the way the screens appear during a basic FireWall-1 installation.

Note: This sample installation shows only those screens necessary for a basic installation.

Installing the Management Software

1. **Begin by inserting the CD into the CD drive and executing the *setup.exe* file. For example:**

   D:\windows\fw1\setup.exe

   The Choose Destination Location window (Figure 1-1) opens.

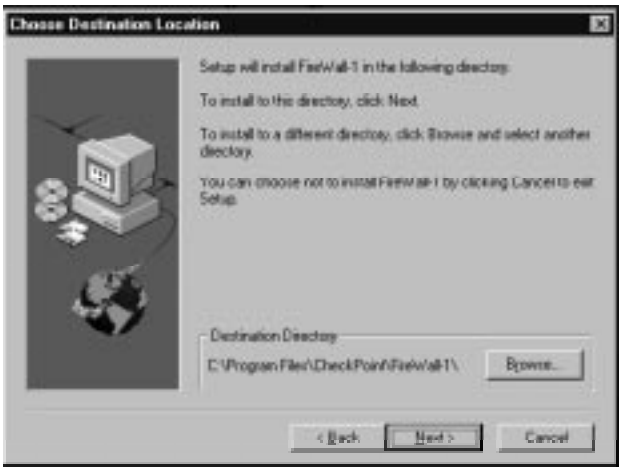
Choose Destination Location
Setup will install FireWall-1 in the following directory.
To install to this directory, click Next.
To install to a different directory, click Browse and select another directory.
You can choose not to install FireWall-1 by clicking Cancel to exit Setup.
Destination Directory
C:\Program Files\CheckPoint\FireWall-1\
Browse...
< Back
Next >
Cancel

Figure 1-1. Choose Destination Location Window

2. **Choose a destination directory. For this sample installation, we accept the default directory.**
3. **Click on Next.**

   The Selecting Product Type window (Figure 1-2) opens.

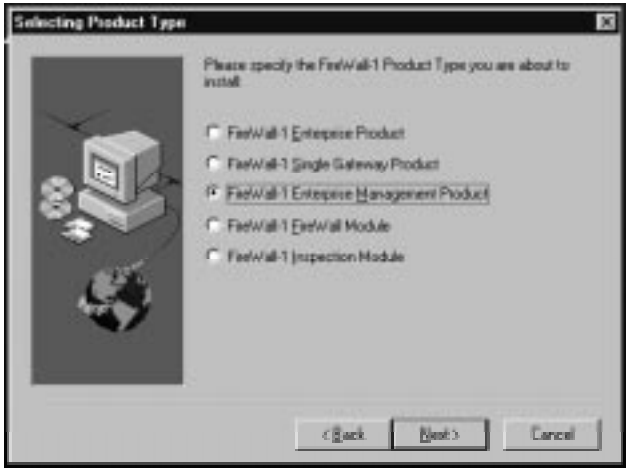
Selecting Product Type
Please specify the FireWall-1 Product Type you are about to install.
FireWall-1 Enterprise Product
FireWall-1 Single Gateway Product
FireWall-1 Enterprise Management Product
FireWall-1 FireWall Module
FireWall-1 Inspection Module
< Back
Next >
Cancel

Figure 1-2. Selecting Product Type Window

4. **Choose the FireWall-1 component you want to install. To be compatible with BaySecure FireWall-1, choose FireWall-1 Enterprise Management Console Product.**
5. **Click on Next.**

   The Licenses window (Figure 1-3) opens.

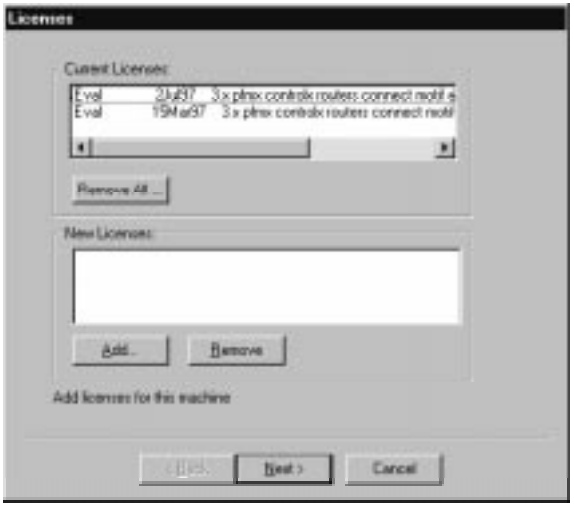

Figure 1-3. Licenses Window

6. **Enter the license information you obtained from Check Point.**
7. **Click on Next.**

The Administrators window (Figure 1-4) opens.

Figure 1-4. Administrators Window

You must specify at least one administrator.

8. **Click on Add.**

   The Add Administrator window (Figure 1-5) opens.

Figure 1-5. Add Administrators Window

9. **Enter the administrator's user name and password, which is limited to eight characters, and a password confirmation, and click on OK. You return to the Administrators window.**

10. **Click on Next.**

    The GUI Clients window opens. Do not enter GUI clients at this time.

11. **Click on Next.**

    The Remote Modules window appears. Do not enter remoter modules at this time.

12. **Click on Next.**

    The Hit Key Session window (Figure 1-6) opens.

Figure 1-6. Hit Key Session Window

13. **Follow the directions in the window and enter random characters, with a delay of a few seconds between them, until the indicator bar is full.**

    Be sure not to type the same character twice in a row and vary the delay between the characters.

14. **Click on Next.**

The CA Key window opens (Figure 1-7).

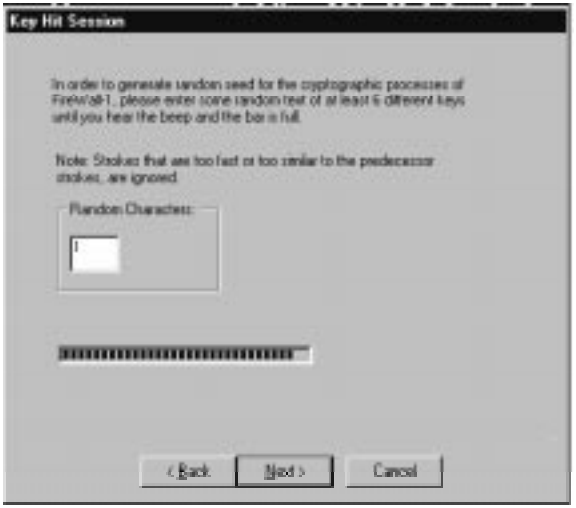

Figure 1-7. CA Key Window

15. **Click on Generate to generate a new key.**

    The host uses the RSA key to generate a digital signal for authenticating its communications in its capacity as a Certificate Authority.

    Generating the key may take several minutes.

16. **Click on Finish.**

Installing the GUI Client

1. **Begin by inserting the CD into the CD drive and executing the *setup.exe* file. For example:**

   `D:\windows\gui_client\disk1\setup.exe`

   The Choose Destination Location window (Figure 1-8) opens.

2. **Choose a destination directory.**

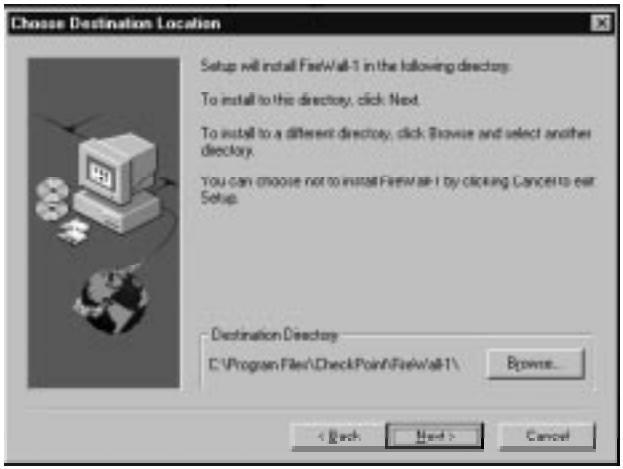
Choose Destination Location
Setup will install FireWall-1 in the following directory.
To install to this directory, click Next.
To install to a different directory, click Browse and select another directory.
You can choose not to install FireWall-1 by clicking Cancel to exit Setup.
Destination Directory
C:\Program Files\CheckPoint\FireWall-1\
Browse...
< Back
Next >
Cancel

Figure 1-8. Choose Destination Location Window

For this sample installation, accept the default directory.

3. **Click on Next.**

The Select Components window (Figure 1-9) opens.

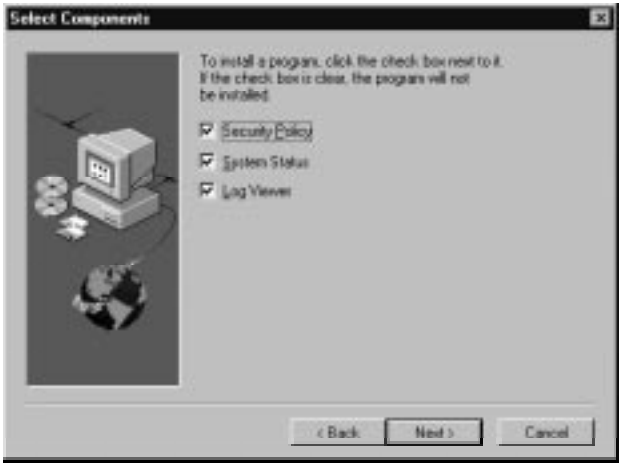
Select Components
To install a program, click the check box next to it. If the check box is clear, the program will not be installed.
Security Policy
System Status
Log Viewer
< Back
Next >
Cancel

Figure 1-9. Select Components Window

4. **Install the Security Policy, System Status, and Log Viewer components by clicking on each item.**

Customizing the FireWall-1 Installation

You can customize your FireWall-1 installation by executing the *FireWall-1 Configuration* file. To execute the file, enter

`D:`**\Start\Programs\FireWall-1\FireWall-1 Configuration**

Using the *FireWall-1 Configuration* file, you can add

- A license
- Administrators
- GUI clients
- Remote modules
- CA keys

Refer to your Check Point documentation for details.

Creating and Configuring a FireWall on the Router

This section explains how to create a firewall on the router using Site Manager.

You can also use the Technician Interface, which lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Before you begin, you must first configure and enable IP on the router and enable TCP on all slots on the router. Refer to *Quick-Starting Routers* for instructions.

Begin by starting Site Manager. Then follow these steps:

1. **Select Configuration Manager in either local, remote, or dynamic mode from the Tools menu.**

   The Configuration Manager window opens (Figure 1-10).

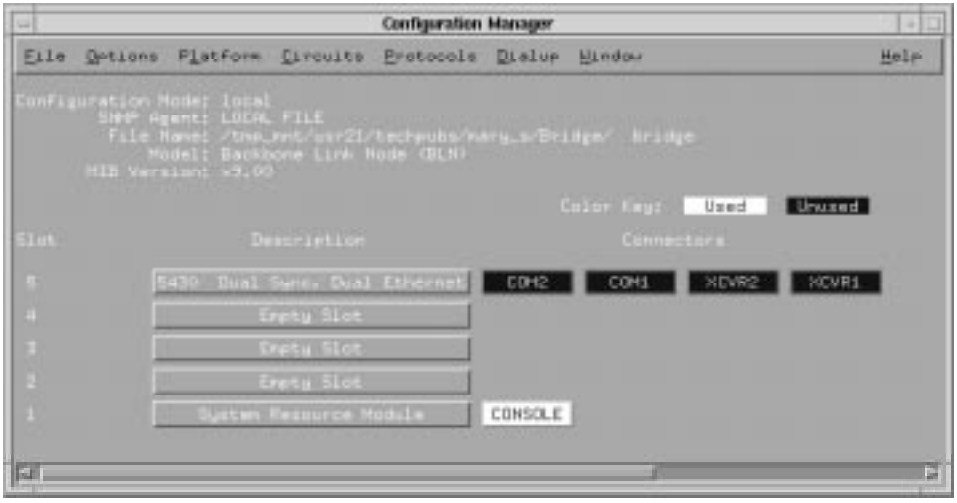

Figure 1-10. Configuration Manager Window

2. **Open a configuration file if local or remote mode is selected.**
3. **Select Protocols > Global Protocols > FWALL > Create.**

   The following confirmation box appears to verify that you have created a firewall on the router.

4. **Click on OK.**

Note: After you create a firewall on the router, you cannot remove it.

5. **To enable the firewall, select Protocols > Global Protocols > FWALL > Global.**

   The F.W. Global window opens (Figure 1-11) to verify that you want to enable a firewall to be active on the router. Click on OK.

Figure 1-11. F.W. Global Window

6. **To configure the firewall, select Protocols > Global Protocols > FWALL > FWALL Router PARAMS.**

   A warning box appears, indicating that you may need to establish a static route between the router and the management station before you configure the parameters.

   If you do not establish a static route and your management station and router are on different subnets, you will be unable to communicate with the router. Refer to *Configuring IP Services* for information about creating a static route.

7. **Click on OK.**

The F.W. Router Parameters window opens (Figure 1-12).

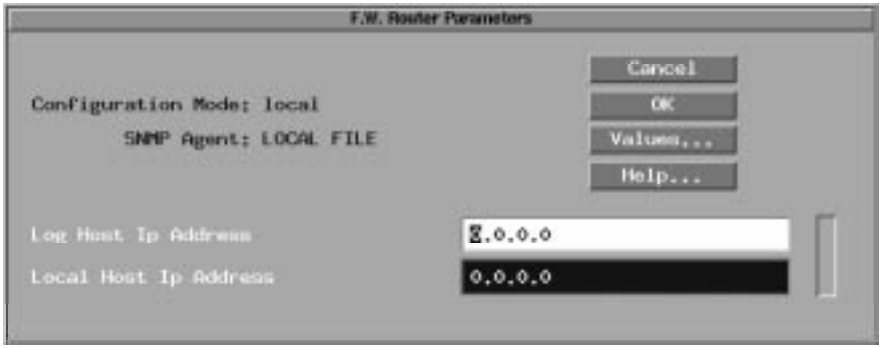

Figure 1-12. F.W. Router Parameters Window

8. Complete the F.W. Router Parameters window.

To configure a firewall, you must supply values for all of the parameters that appear in the F.W. Router Parameters window. Refer to the parameter descriptions that follow. When you finish configuring the parameters, click on OK to make all parameter settings take effect.

Parameter:	**Log Host IP Address**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Shows the IP address of the host on which you installed the FireWall-1 management software. This host becomes the firewall management station, from which you control the firewall. The management station also logs all violations of the security rule base.
Instructions:	Enter the IP address of the host where you installed the control module. If the log host IP address and the local host IP address you specify are on different subnets, then you must configure a static route to the local host IP address to enable communication between the router and the management station. *Configuring IP Services* provides information about configuring a static route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.11.2.4

Parameter:	**Local Host IP Address**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Shows the IP address of the router on which the firewall resides.
Instructions:	Enter the IP address of the host where you installed the firewall module. If the log host IP address and the local host IP address you specify are on different subnets, then you must configure a static route to the local host IP address to enable communication between the router and the management station. *Configuring IP Services* provides information about configuring a static route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.11.2.6

Enabling the FireWall on All Router Interfaces

After you have created a firewall on the router, you can enable it on all interfaces by selecting **Protocols > Global Protocols > FWALL > Interfaces** from the Configuration Manager window.

The FW on ALL Interfaces window (Figure 1-13) opens to verify that you enabled the firewall on all interfaces.

Figure 1-13. FW on ALL Interfaces Window

Click on OK to enable the firewall on all router interfaces. Otherwise, click on Cancel.

When you click on OK, a message box opens, confirming that you are enabling the firewall on all interfaces.

Once you enable the firewall on all interfaces and reboot the router, you will not be able to communicate with the router through Site Manager until you change the FireWall-1 default security policy.

Caution: If your firewall management station and router are on different subnets, you will not be able to communicate with the router from the management station unless you establish a static route from the management station to the router before you activate the firewall. Refer to *Configuring IP Services* for information about creating a static route.

Activating the Firewall

Before the FireWall-1 security policy will take effect on the router, you must first activate the firewall by booting the router. Booting a router warm-starts every processor module in the router. Pressing the Reset button on the front panel of the router performs the same procedure.

Note: When you activate the firewall, the default security policy prevents all interfaces supported by the firewall from communicating with the router. If the firewalled router and management station are on different subnets, you must establish a static route to enable communication between the router and the management station before you activate the firewall. For information about configuring a static route, refer to *Configuring IP Services.*

Use the Administration menu to reboot the router.

1. **From the main Site Manager window, select Administration > Boot Router.**

The Boot Router window opens (Figure 1-14).

Figure 1-14. Boot Router Window

2. **Specify the correct volume and boot image.**
3. **Select the correct router volume and configuration file. Then click on Boot.**

   A confirmation window appears.
4. **Click on OK in the confirmation window and wait a few minutes to give the router time to reboot.**
5. **Select View > Refresh Display from the main Site Manager window to verify that the router booted correctly.**

If the router booted correctly, system information appears in the main Site Manager window.

If the router did not boot correctly, system information does not appear. In this case, make sure that you followed the procedures described in this section.

If you have any questions, refer to *Configuring and Managing Routers with Site Manager* or call your local Bay Networks Technical Solutions Center.

Configuring a FireWall Security Policy

A security policy is a collection of rules that define the way the firewall operates. Check Point supplies a default security policy that drops all attempts at communication with the router. This security policy goes into effect when you first activate the firewall on the router.

You must define a security policy that explicitly defines acceptable communication to the router, based on the source address, destination address, and type of service. Refer to your Check Point FireWall-1 documentation for details about how to configure a security policy.

Installing the Security Policy on the Router

Once you have defined a security policy, you must install it on the router. Installing a security policy means downloading it to the firewalled objects that will enforce it.

When you download the security policy, the FireWall-1 software

- Verifies that the rule base is logical and consistent
- Generates an inspection script from the rule base
- Compiles the inspection script to generate inspection code for the router
- Downloads the inspection code to the router

For information about how to install the security policy, refer to your Check Point documentation.

Troubleshooting Checklist

If you experience problems with FireWall-1, verify that you have performed these steps:

- Enabled TCP on all slots on the router
- Created a firewall using Site Manager
- Created a static route if the router and firewall management stations are on different subnets
- Rebooted the router with a firewall configuration file
- Synchronized the router and management station passwords by executing the **fwputkey** command on both the router and the firewall management station
- Defined a security policy and added a network object for the router using the FireWall-1 GUI
- Saved the configuration and booted the router
- Installed the security policy on the router

If you have performed these steps and are still having system problems, contact your Bay Networks Technical Solutions Center.

Index

A

activating FireWall-1, 1-22
adding
  administrators, 1-8
  groups, 1-8
  GUI clients, 1-8, 1-17
  license, 1-8, 1-17
  remote modules, 1-8, 1-17

B

Bay Networks Press, xiii
booting the router, 1-22

C

Check Point, contacting, 1-2
commands
  commit, 1-17
  fw putlic, 1-9
  fwconfig, 1-8
  fwinstall, 1-4
  fwputkey, 1-9
  fwstart, 1-9
  fwstop, 1-9
  fwui&, 1-10
  set, 1-17
Configuration Manager, 1-18
configuring a firewall, 1-17
control module, defined, 1-1
creating a firewall, 1-17
customer support
  programs, xiii
  Technical Solutions Centers, xiv

D

daemons, 1-9

E

enabling a firewall, 1-21
extracting tar files, 1-3

F

firewall module, 1-1
FireWall-1 License, obtaining, 1-2
fw putlic command, 1-9
fwconfig command, 1-8
fwinstall command, 1-4
fwputkey command, 1-9
fwstart command, 1-9
fwstop command, 1-9
fwui& command, 1-10

G

groups, adding, 1-8
GUI clients, adding, 1-8, 1-17

I

inspection code, 1-24
installation
  options, 1-4
  sample, 1-5, 1-10

installing management software, 1-4

L

license
adding, 1-8, 1-17
installing on management station, 1-9
obtaining, 1-2
Local Host IP Address parameter, 1-21
Log Host IP Address parameter, 1-20

M

modules
control, 1-1
firewall, 1-1
mounting a CD drive, 1-3

P

publications
ordering, xiii

R

refreshing the display, 1-23
remote modules, adding, 1-8, 1-17
Reset button, 1-22
rule base, verifying, 1-24
rules, defined, 1-24

S

security policy
configuring, 1-24
downloading, 1-24
serial number, obtaining, 1-2
starting the daemons, 1-9
static route, 1-22
synchronizing the router and management station, 1-9

T

tar files, extracting, 1-3
Technical Solutions Centers, xiv
Technician Interface, 1-17